Kontinuasjonseksamen i 11174 Datasikkerhet

20. august 2002

Eksamen består av 5 oppgaver over 2 sider. Total poengsum: 200

Faglig kontakt under eksamen: Martin Gilje Jaatun, tlf. 900 26 921

OPPGAVE 1 – OPPVARMING

a) Hva regnes som de tre grunnpilarene i datasikkerhet? (kort) (6 poeng)
b) Hva menes med monoalfabetisk substitusjon? (kort) (4 poeng)
c) Hvordan knekkes et monoalfabetisk substitusjonschiffer? (kort) (6 poeng)
d) Hva menes med polyalfabetisk substitusjon? (kort) (4 poeng)
e) Hva er Kerchoffs prinsipp? (kort) (6 poeng)

OPPGAVE 2 – SYMMETRISK KRYPTOGRAFI

a) Hva er en S-boks? (kort) (4 poeng)
b) Hvor mange bit er det i en DES-nøkkel? (kort) (4 poeng)
c) Hva menes med "blokkstørrelse" i et blokkchiffer? (kort) (6 poeng)
d) Hva er blokkstørrelsen i DES? (kort) (4 poeng)
e) Tenk deg at du DES-krypterer en klartekst X med alle mulige nøkler, og kaller denne mengden av chiffertekster for Y. Hvis du DES-krypterer klarteksten *to* ganger med to forskjellige nøkler, får du da en chiffertekst som ikke finnes i Y? Begrunn svaret kort. (6 poeng)
f) Forklar hvordan man kan utføre et Meet-in-the-middle-angrep på Double-DES. (12 poeng)
g) Omtrent hvor stor arbeidsmengde krever et Meet-in-the-middle-andrep på Double-DES sammenlignet med uttømmende søk ("brute force") gjennom alle (single-)DES-nøkler? (kort) (6 poeng)

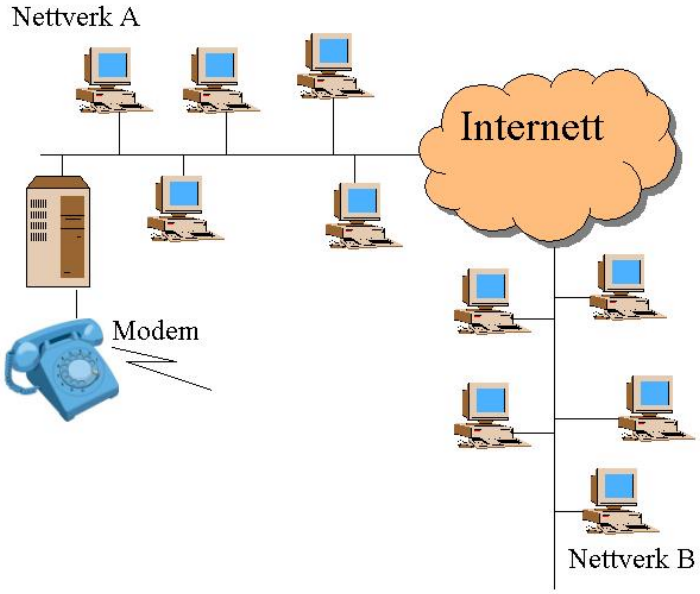
OPPGAVE 3 – ASYMMETRISK KRYPTOGRAFI

a) Hvor mange nøkler (og av hvilken type) kreves totalt for at Alice og Bob skal kunne kommunisere sikkert ved hjelp av asymmetrisk kryptografi? (kort) (6 poeng)
b) I RSA har vi at kryptering skjer ved $C = P^e \pmod n$ og dekryptering ved at $P = C^d \pmod n$. Vis ved innsetting og Eulers teorem at det siste uttrykket stemmer. (12 poeng)
c) Flere steder i litteraturen settes det likhetstegn mellom "signering" og "kryptering med privat nøkkel". Hvorfor er dette uheldig? (6 poeng)

OPPGAVE 4 – SIKKERHETSAPPLIKASJONER

a) Tegn en figur og forklar hvordan PGP signerer og krypterer en melding som skal sendes fra Alice til Bob. (12 poeng)
b) Forklar hensikten med PGPs "web of trust", og skissér hvordan det virker i praksis. (12 poeng)
c) Skissér aktørene i SET (med den forenklingen at vi antar at kortselskap, bank, etc. opptrer som én entitet), og angi hvilke som trenger et sertifikat. (12 poeng)
d) Hvilke sikkerhetsfordeler innebærer SET? (12 poeng)
e) Hvordan beregnes SETs "dual signature", og hvordan brukes den? (12 poeng)

OPPGAVE 5 – CASE



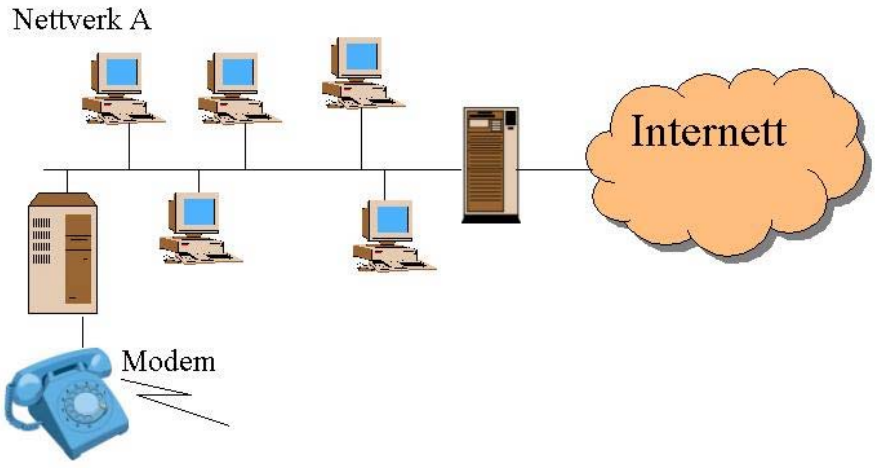
Figur 1: Bedrift med to avdelingskontor

a) Hvilke to teknikker kan man bruke for å skjule de interne adressene til Nettverk A i Figur 1 når maskinene her kommuniserer med internett? (kort) (6 poeng)

b) Diskuter forskjeller mellom de to teknikkene i a). (12 poeng)

c) Anta nå at Nettverk A og Nettverk B i Figur 1 er to avdelingskontorer i samme firma. Hvilken teknologi er naturlig å bruke for å knytte disse nettene sammen på en sikker måte over internett? (6 poeng)

d) Hvis vi antar at den fysiske avstanden mellom nettene er så stor at det er upraktisk å manuelt bytte nøkler til stadighet, hvordan kan de to nettene få etablert symmetriske sesjonsnøkler? (12 poeng)



Figur 2: Nettverk beskyttet av brannmur

e) Anta nå at nettverk A er sikret med plassering av en brannmur på overgangen til Internett som vist i Figur 2, og at denne brannmuren har ansvaret for å implementere bedriftens sikkerhetspolicy for trafikk både til og fra Internett. Påpek ved å studere figuren ett moment som bidrar til å undergrave en slik sikkehetspolicy, og foreslå hvordan dette kan utbedres. (12 poeng)